



NIST Special Publication 800-160, Volume 2

# Developing Cyber Resilient Systems

*A Systems Security Engineering Approach*

**NIST**

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

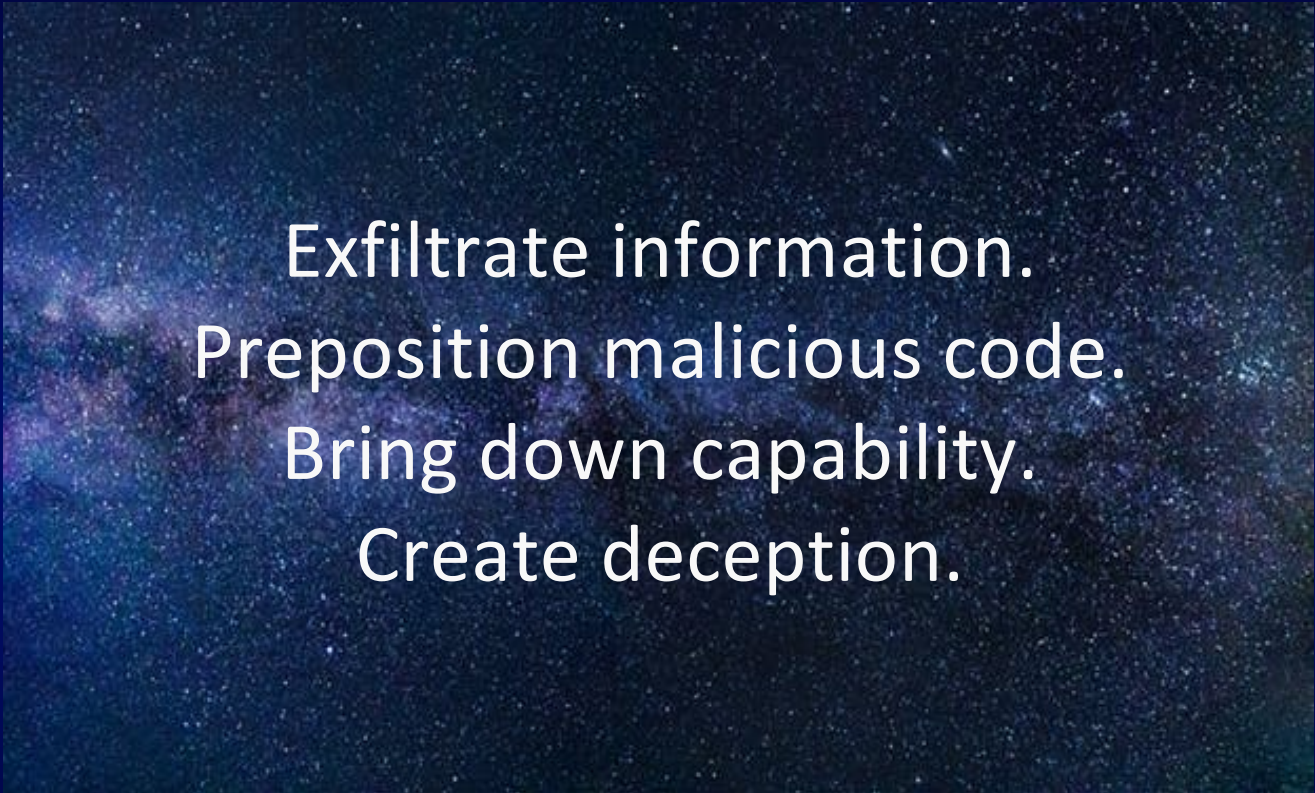


*The Current Landscape...*

Today's systems are very brittle, rely on a one-dimensional protection strategy of penetration resistance, and are highly susceptible to devastating cyber-attacks.

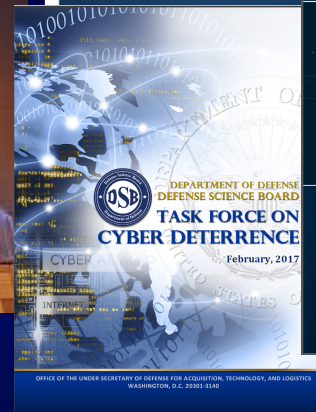
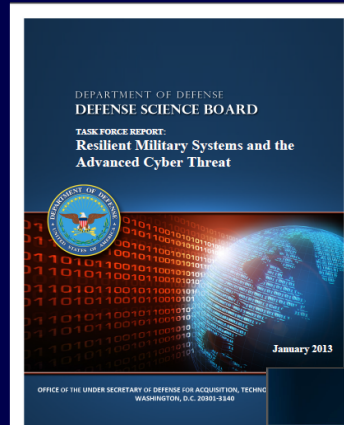


The adversaries are relentless.



Exfiltrate information.  
Preposition malicious code.  
Bring down capability.  
Create deception.

- Resilient Military Systems and the Advanced Cyber Threat
  - Cyber Supply Chain
  - Cyber Deterrence



## Defense Science Board Reports



# Defending cyberspace in 2020 and beyond.



*The Objective...*

Expand the cyber aperture to a multi-dimensional protection strategy that includes developing damage limiting system architectures and cyber resilient systems.



*A New Paradigm...*

Cyber resilient systems operate more like the human body than a traditional finite state computing machine.



## Cyber Resiliency Engineering

An emerging specialty systems engineering discipline, applied in conjunction with resilience engineering and systems security engineering to develop survivable, trustworthy systems.

## Cyber Resiliency.

The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.

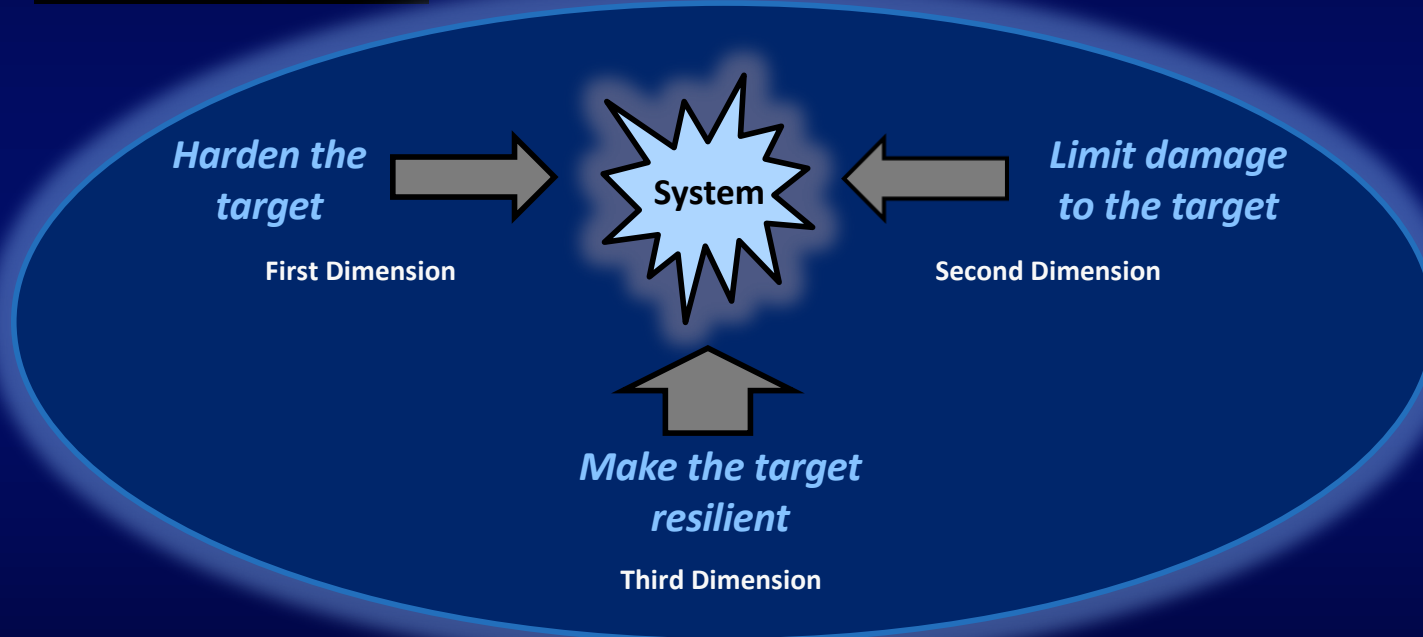


Cyber resiliency relationships with other specialty engineering disciplines.





Reducing susceptibility to *cyber threats* requires a multidimensional strategy.



# Cyber Resiliency and Security in the System Life Cycle.



**ISO/IEC/IEEE 15288:2015**  
*Systems and software engineering*  
— *System life cycle processes*

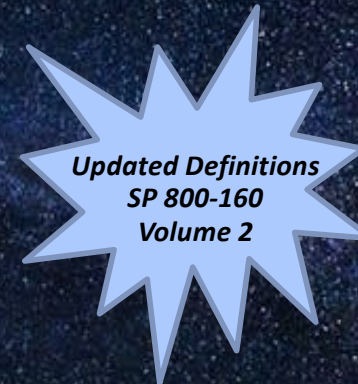


- Business or mission analysis
- Stakeholder needs and requirements definition
  - System requirements definition
    - Architecture definition
      - Design definition
        - System analysis
          - Implementation
          - Integration
        - Verification
        - Transition
      - Validation
    - Operation
    - Maintenance
    - Disposal

**NIST**  
**SP 800-160**  
**Volume 1**

## *Cyber Resiliency Constructs...*

- Goals
- Objectives
- Sub-Objectives
- Techniques
- Approaches
- Strategic Design Principles
- Structural Design Principles



*Bridging Two Communities...*

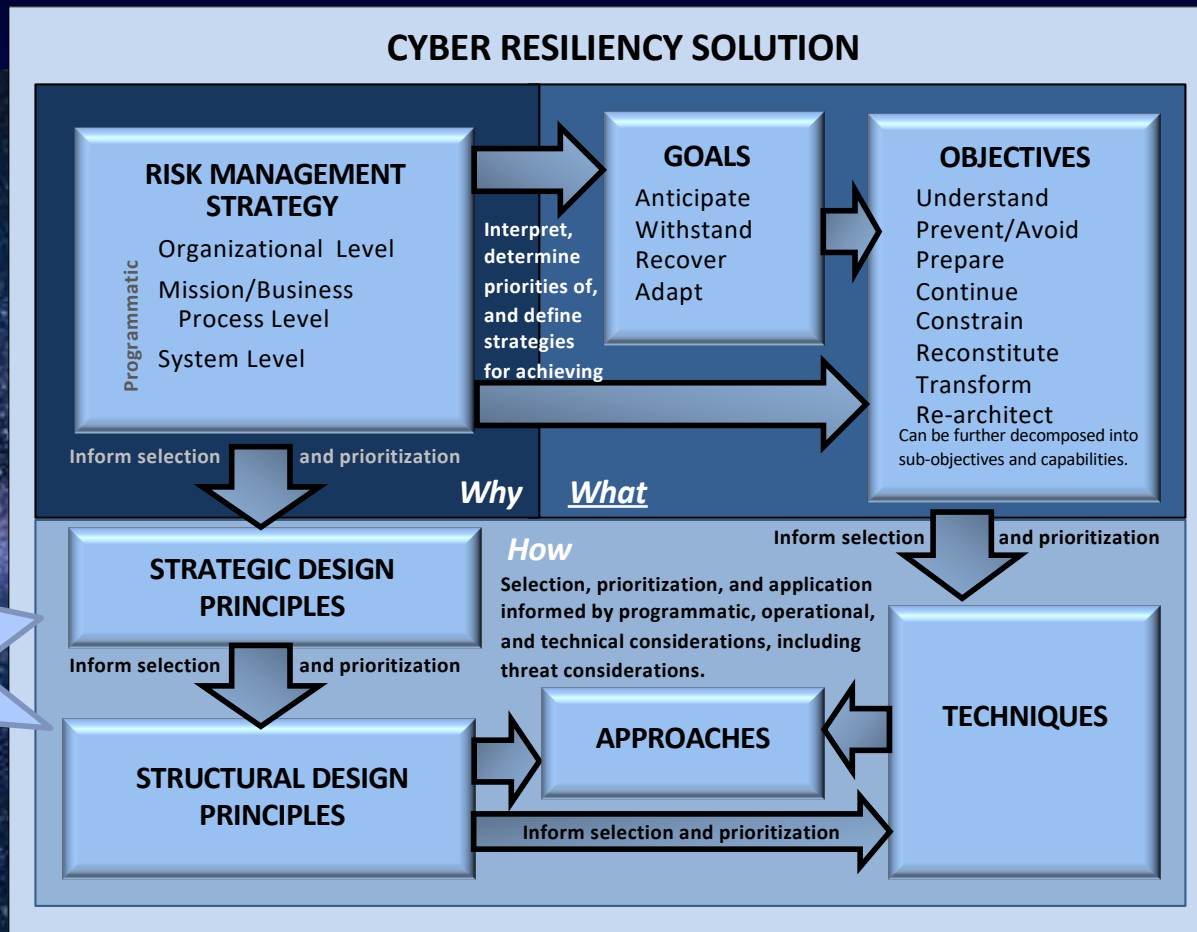
**Systems  
Security  
Engineering**



**Risk  
Management  
Framework**

*Relationship  
Among Cyber  
Resiliency  
Constructs...*

Linkage of  
constructs  
captured in a  
series of tables





## Coverage Analysis

- Provides a mapping of the NSA/CSS Technical Cyber Threat Framework (NTCTF) against the cyber resiliency techniques and approaches.
  - Each of the 21 NTCTF adversary *objectives* is mapped against each of the 48 cyber resiliency approaches.
  - Illustrates how cyber resiliency techniques and approaches can affect threat events using the NTCTF.
  - Mapping identifies which, if any, of 15 effects on the adversary are applicable.

## Sample Coverage Analysis

TECHNIQUE	STAGE →	PRESENCE					
	OBJECTIVE →	Execution	Internal Recon	Privilege Escalation	Credential Access	Lateral Movement	Persistence
	APPROACH						
Redundancy	Protected Backup	No effect	No effect	No effect	No effect	No effect	No effect
	Surplus Capacity	No effect	No effect	No effect	No effect	No effect	No effect
	Replication	No effect	No effect	No effect	No effect	No effect	No effect
Segmentation	Predefined Segmentation	Contain Delay	Contain Delay	Delay Negate Contain	Contain Delay Preempt	Delay Contain	No effect
	Dynamic Segmentation	Contain Delay	Contain Delay	Delay Negate Contain	Contain Delay Preempt	Delay Contain	No effect
Substantiated Integrity	Integrity Checks	Detect	No effect	No effect	No effect	No effect	Detect
	Provenance Tracking	No effect	No effect	No effect	No effect	No effect	No effect
	Behavior Validation	Detect	No effect	Detect	Detect	No effect	Detect
Unpredictability	Temporal Unpredictability	Preempt Detect Delay	Delay Preempt	Delay Preempt	Delay Preempt	Delay Preempt	Delay Preempt
	Contextual Unpredictability	Preempt Detect Delay Exert	Delay Exert Preempt	Delay Exert Preempt	Delay Exert Preempt	Delay Exert Preempt	Delay Exert Preempt

## *Use Cases*

- Provides several cyber resiliency use cases.
  - Self-driving car — Enterprise IT — Campus micro-grid
- Discusses representative situations in which cyber resiliency is considered by systems security engineering.
- Shows how cyber resiliency concepts and constructs can be interpreted and applied to that situation.
- Illustrates how cyber resiliency solutions can be defined or how specific solutions can be applied.

## Real World Example: Ukraine Power Grid Attack

MALWARE FUNCTIONALITY	POTENTIAL MITIGATIONS	REPRESENTATIVE TECHNOLOGIES
Execute SIPROTEC DoS, HMI switch toggle, Amplify, Data Wiper attacks	<ul style="list-style-type: none"> <li>• <a href="#">Redundancy</a> with <a href="#">Diversity</a> of HMIs [impede]</li> <li>• <a href="#">Analytic Monitoring</a> of HMI interactions with operators, and to detect Wiper commands and derivatives in the scheduler [expose]</li> <li>• <a href="#">Adaptive Response</a> (e.g., run notepad to remove Wiper commands and derivatives) [impede, limit]</li> </ul>	<ul style="list-style-type: none"> <li>• Make architectural changes to use existing technologies in a diverse and redundant way</li> <li>• IDS for OT, ICS, or SCADA</li> </ul>
Future Payloads	<ul style="list-style-type: none"> <li>• <a href="#">Redundancy</a> with <a href="#">Diversity</a> of OT procedures and protocols [impede]</li> <li>• <a href="#">Redundancy</a> of actions/logins on HMIs [impede]</li> </ul>	<ul style="list-style-type: none"> <li>• Make architectural changes to use existing technologies in a diverse and redundant way</li> <li>• Use an OT security management platform to require redundant actions via HMIs</li> </ul>

For each step of attack, identifies potential cyber resiliency mitigations and representative technologies.



NIST Special Publication 800-160, Volume 2  
**Developing Cyber Resilient Systems**  
*A Systems Security Engineering Approach*

**Final Public Draft**

**Comment Period: September 4 through November 1**

Comments to: [sec-cert@nist.gov](mailto:sec-cert@nist.gov)



100 Bureau Drive Mailstop 7770  
Gaithersburg, MD USA 20899-7770

**Email**

[ron.ross@nist.gov](mailto:ron.ross@nist.gov)

**LinkedIn**

[www.linkedin.com/in/ronrossecure](http://www.linkedin.com/in/ronrossecure)

**Web**

[csrc.nist.gov](http://csrc.nist.gov)

**Mobile**

301.651.5083

**Twitter**

[@ronrossecure](https://twitter.com/ronrossecure)

**Comments**

[sec-cert@nist.gov](mailto:sec-cert@nist.gov)